

FIG.1

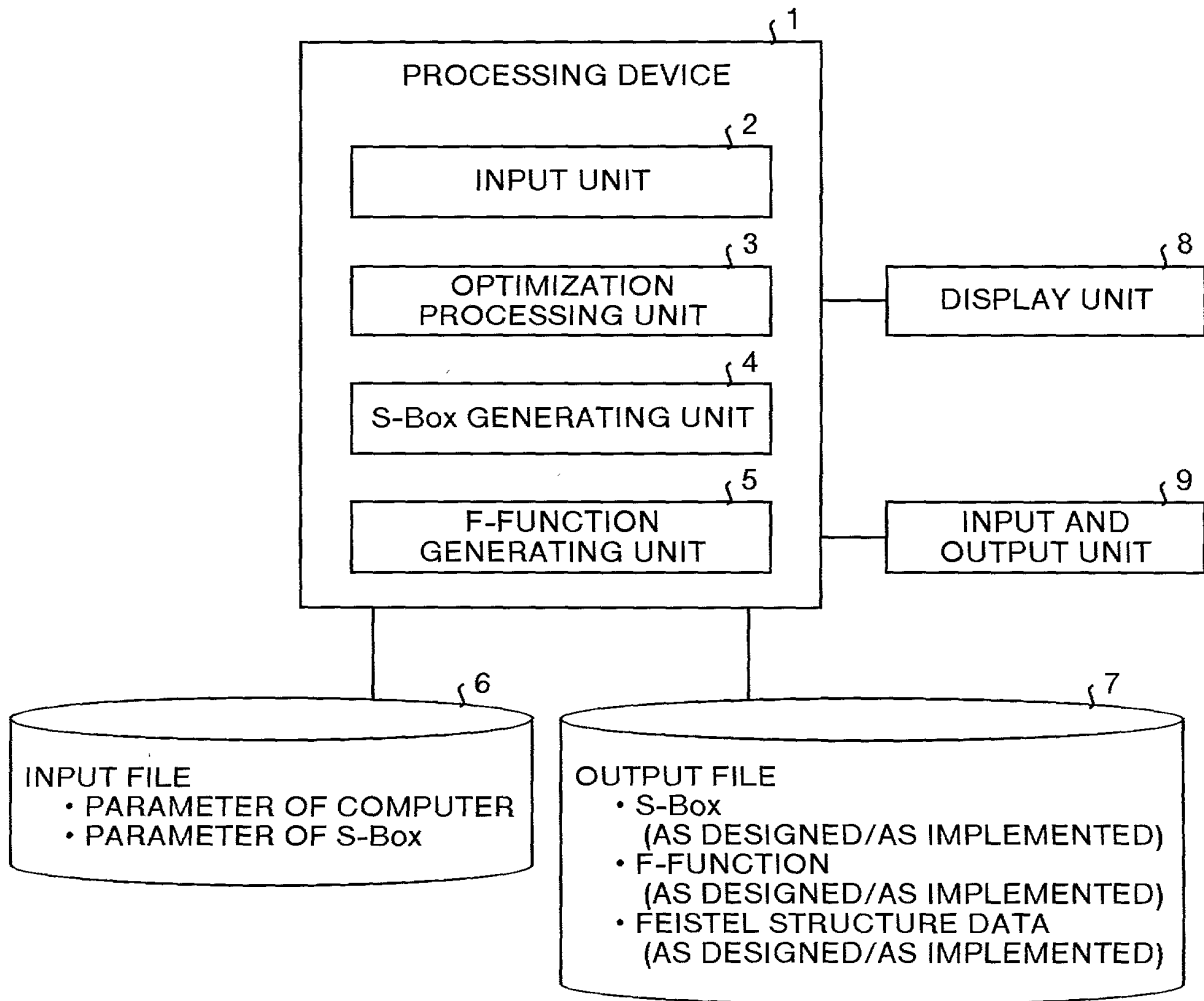
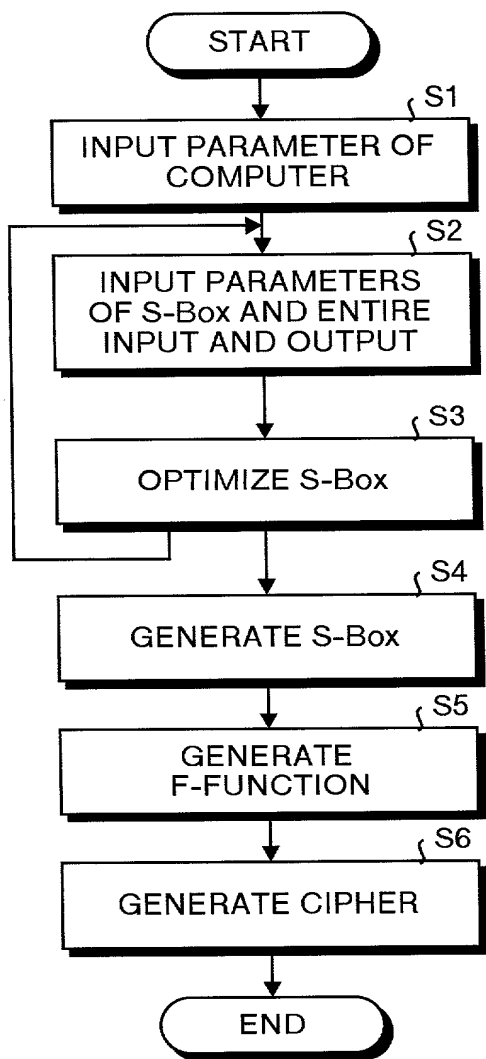


FIG.2



MEMORY CAPACITY OF PRIMARY CACHE
 (1) Pentium II PROCESSOR-16 KBYTES
 (2) PA-RISC PROCESSOR-1 MBYTE

- INPUT AND OUTPUT NUMBER OF S-Box IS 5 BITS OR MORE
- ENTIRE INPUT AND OUTPUT NUMBER IS 32 BITS

(1) 32 → 6, 5, 5, 5, 5, 6
 └─┘ └─┘ └─┘
 11 10 11

(2) 32 → 6, 5, 5, 5, 5, 6
 └─┘ └─┘
 16 16

- GENERATE SECRET KEY RELATED TO F-FUNCTION KEY HAVING THE SAME BIT NUMBER AS F-FUNCTION INPUT AND OUTPUT BIT NUMBER

FIG.3

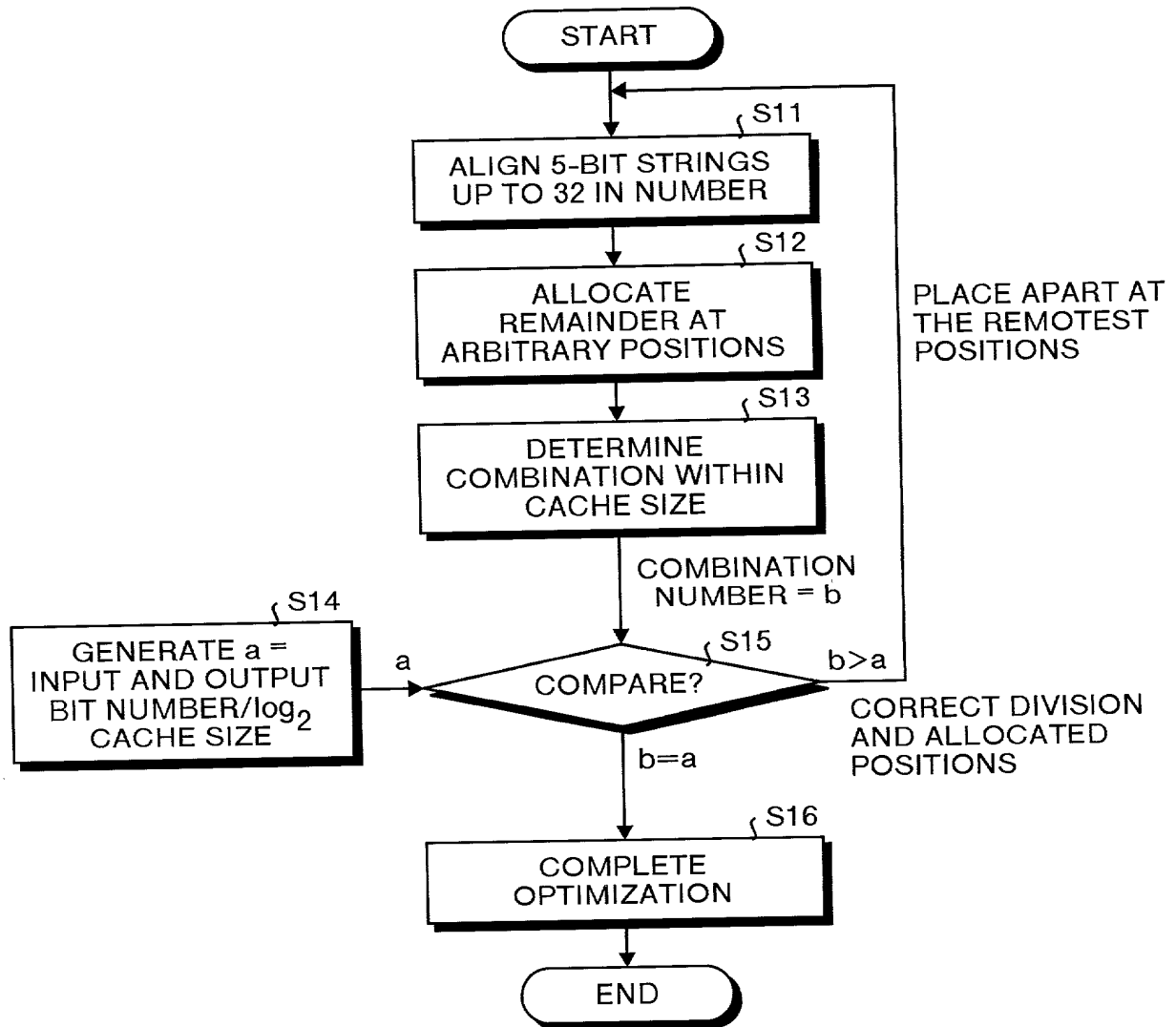


FIG.4

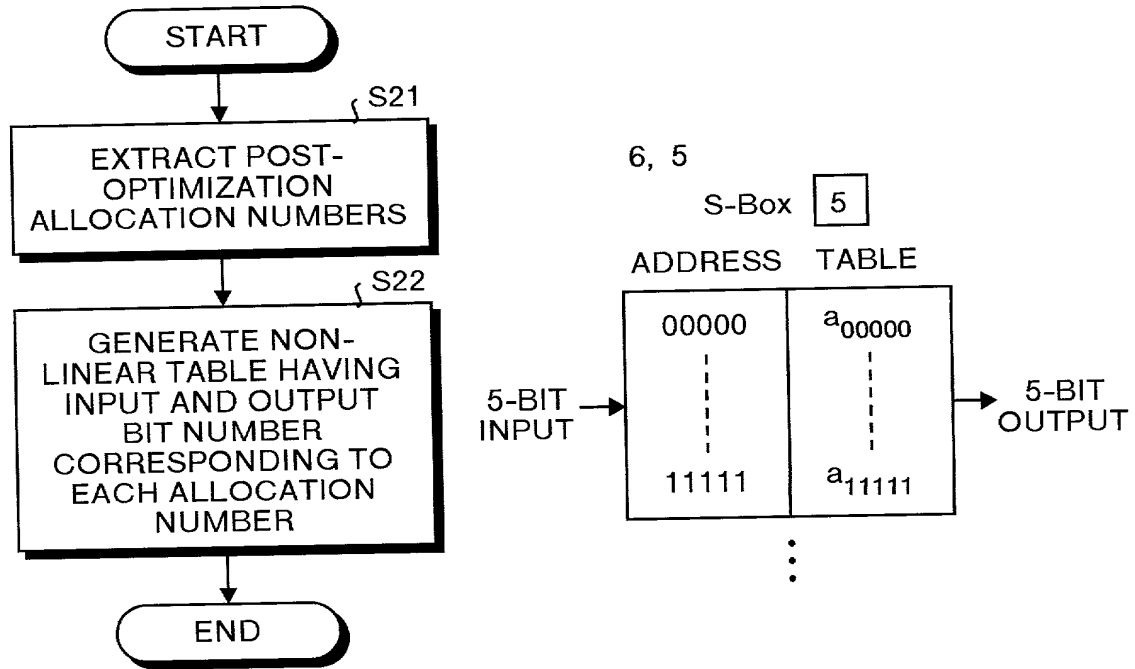


FIG.5

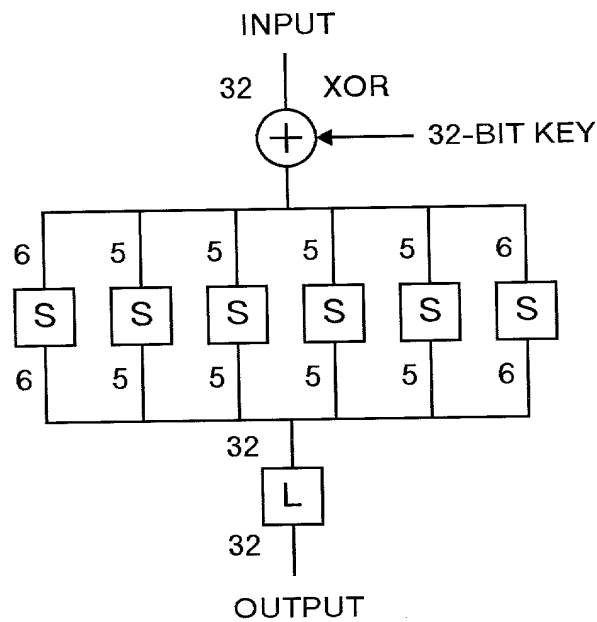


FIG.6

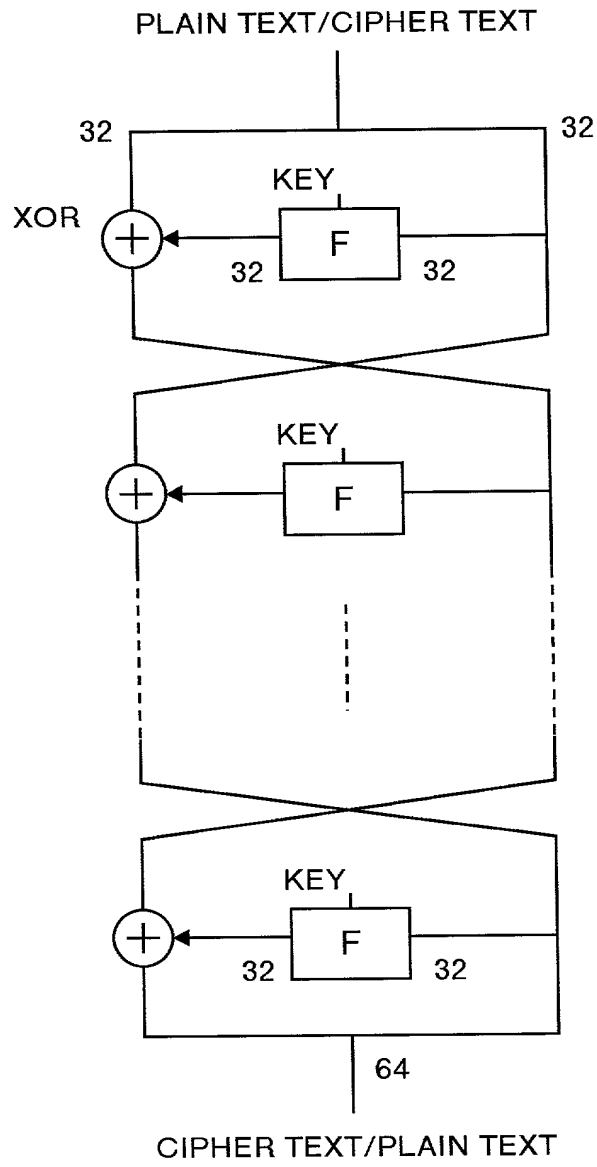
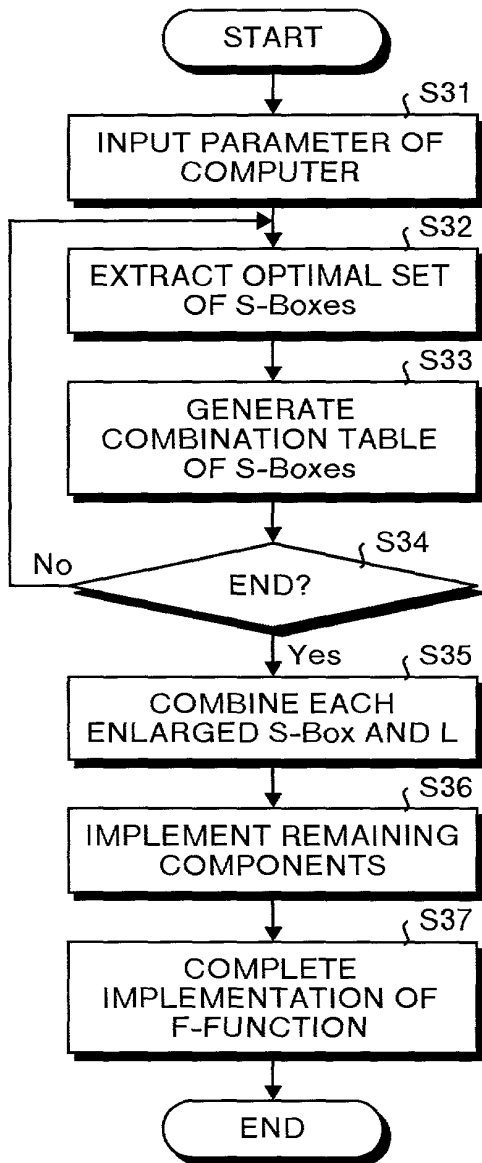
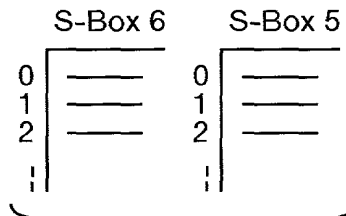


FIG.7

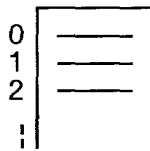


MEMORY CAPACITY OF PRIMARY CACHE
Pentium II PROCESSOR-16 KBYTES

6 5 5 5 6
(6, 5)



S-Box 11



ENLARGED S-Box

- KEY ADDER UNIT
- INPUT AND OUTPUT UNIT

⋮

FIG.8

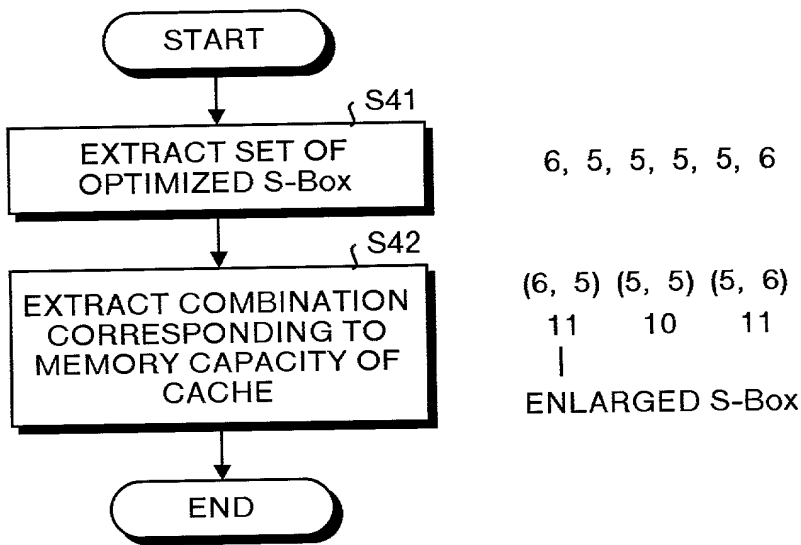


FIG.9

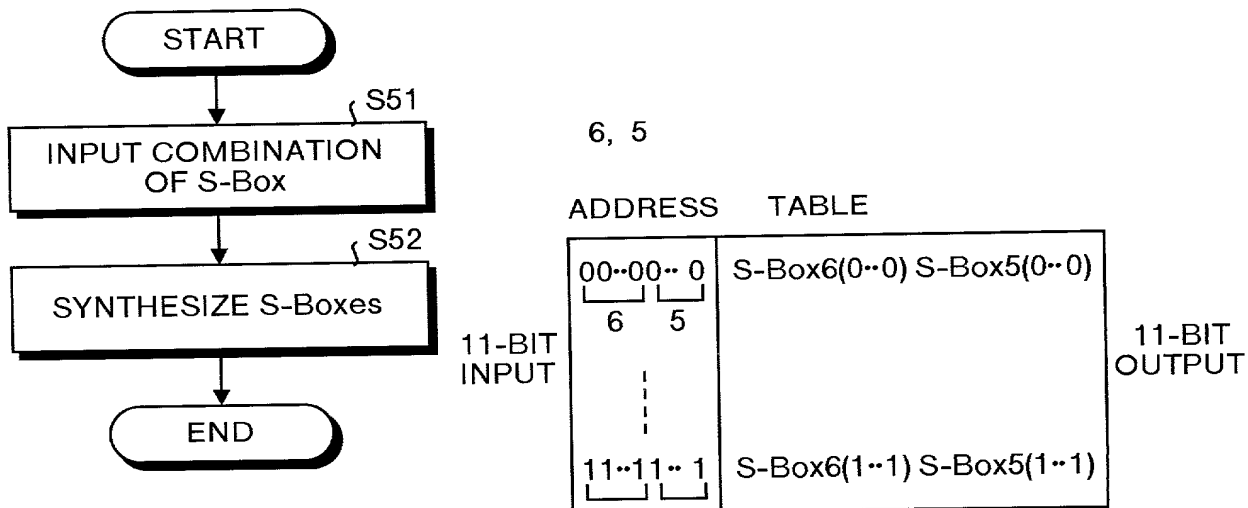


FIG.10

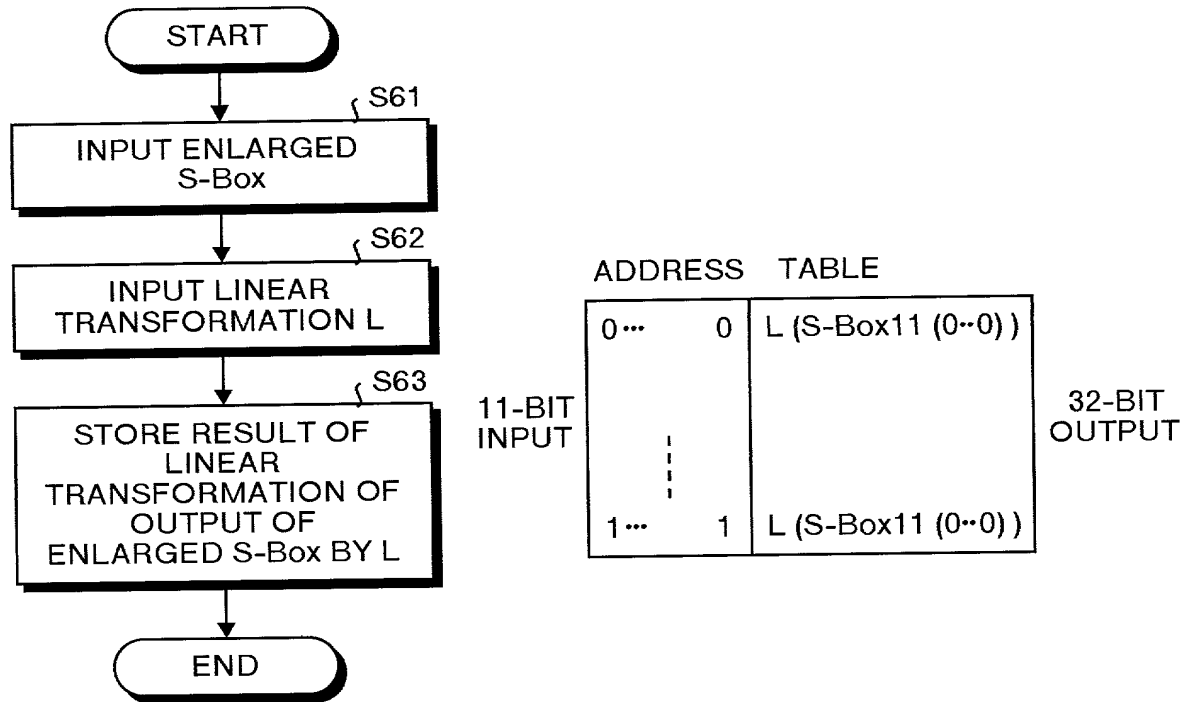


FIG.11

